CONVERGENCIA COBIT 5.0 DE 2012 FRENTE A LEY SARBANES -OXLEY

Niño Joan Sebastián
ingsebastianino@gmail.com
Universidad Piloto de Colombia

Resumen—En la actualidad se evidencia como las organizaciones y sus ejecutivos están haciendo esfuerzos para mantener información valiosa, para apoyar las decisiones del negocio y así generar valor comercial por la tecnología de la información (TI), es decir: lograr mejoras al negocio y cumplir las metas estratégicas mediante el uso innovador de las tecnologías de la información, y así, lograr mantener el riesgo relacionado con TI a niveles aceptables. Este trabajo tiene como resultado fortalecer el conocimiento y enunciar la convergencia de las mejores prácticas de CoBIT 5.0 de 2012 frente a la ley Sarbanes-Oxley frente a las empresas que cotizan en la bolsa de valores, evitando de este modo que las acciones de las mismas sean modificadas o alteradas de forma sospechosa.

Abstract—This work results in the knowledge and communication of the best practices of CoBIT 5.0 of 2012 against the Sarbanes-Oxley law against the companies listed on the stock exchange, preventing the actions of the same from being modified or altered from suspicious form.

Índice de Términos—Amenaza, confidencialidad, disponibilidad, integridad, impacto, CoBIT 5.0, ISACA, riesgo, vulnerabilidad, Sarbanes-Oxley, convergencia, buenas prácticas, conocimiento, businessprocess, COSO.

I. INTRODUCCIÓN

En la actualidad las malas prácticas en el aseguramiento de un sistema de información en la infraestructura Tecnológica de una compañía, muestran las principales vulnerabilidades en el aseguramiento de la información.

El artículo tiene como resultado unir y dar lo mejor de las buenas prácticas del Framework CoBIT 5.0 frente a la ley Sarbanes-Oxley, asimismo lograr el valor para las partes interesadas en la organización en el cuál se requiere un buen gobierno y de la misma forma una administración de los activos de TI. Adicional este documento da a conocer los lineamientos y capacidades que se deben seguir incorporando en el gobierno de TI frente a los requerimientos legales cómo de cumplimiento regulatorio y contractual de la ley Sarbanes-Oxley.

II. ESTABLECIMIENTO DE CONTEXTO

La guía de mejores prácticas CoBIT 5.0, ayuda a las organizaciones a nivel mundial a crear un valor óptimo a partir de las tecnologías de la información, entre su realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos que están disponibles.

De esta forma, CoBIT 5.0 permite que las tecnologías de la información estén relacionadas se gobiernen y administren de una manera eficaz y holística comprendiendo toda la organización y sus partes externas, esto incluye el alcance completo de la organización, incluyendo todas las áreas de responsabilidad funcionales y de negocios involucrando todo el ámbito de tecnologías de la información. Estos principios y guías de CoBIT 5.0 son útiles para cualquier organización, sea pública y privada.

Los principios de CoBIT 5.0 son los siguientes:

1) Satisfacer las necesidades de las partes interesadas.
2) Cubrir la organización de forma integral.
3) Aplicar un sólo marco integrado.
4) Habilitar un enfoque holístico.
5) Separar el gobierno de la administración

Se tiene en cuenta los principios de CoBIT 5.0 para poder realizar su convergencia requerida. Se utiliza el marco de referencia frente a la ley Sarbanes-Oxley en el cuál se debe tener alineado los objetivos del negocio, asimismo a la necesidad que requiere las organizaciones para salvaguardar sus bienes, acciones o simplemente su reputación por medio de procedimientos y controles preestablecidos.

Fig. 1. Principios de CoBIT 5.0
Fuente: CoBIT 5.0 ® 2012 ISACA All Right Reserved

La legislación Sarbanes-Oxley llega a medio oriente, Japón, Sudáfrica, Canadá y Europa, por lo tanto, los marcos de esta forma se vuelven mucho más importantes para documentar y probar la efectividad de los controles internos que se tienen en las organizaciones a nivel mundial. Dentro de

las diferencias: Los auditores externos no están obligados a dar testimonio de la certificación en cuánto a la administración sobre los controles internos en Canadá.

Se debe tener un grupo de trabajo para la revisión de equipos financieros, empresariales y controles de procesos de negocio automatizados de tal forma que se relacione con CoBIT 5.0 en temas de procesos, estructuras organizacionales, cultura, ética y comportamiento, hasta principios, políticas y marcos dando alcance a información, servicios, infraestructura y aplicaciones y su principal enfoque serían las personas, habilidades o competencias formando de esta forma un conjunto de óptimos profesionales llamados recursos como se muestra en la Fig.1, en el cuál estan descritos los cinco principios del marco de referencia.

Se debe tener claro que para la convergencia Sarbanes-Oxley y CoBIT 5.0, asimismo la necesidad del negocio, objetivos específicos y generales de la organización, y de este modo poder conocer las necesidades frente a las partes interesadas dentro del gobierno de tecnologías de la información.

Es fundamental tener en claro la información transmitida en cualquier organización que constituye un recurso claro para todas las partes, esta a su vez se crea, usa, retiene, divulga y se destruye, a nivel mundial las tecnologías de la información juegan un papel clave en todas las actividades.

La tecnología se está convirtiendo en parte integral de todos los aspectos de la vida personal y comercial, para poder involucrar y alternar CoBIT 5.0 con Sarbanes-Oxley es necesario manejar unos habilitadores involucrando una mejora continua dentro de los mismos, a continuación, se evidencia los siete pasos que describe ISACA para el tema de establecimiento de contexto.

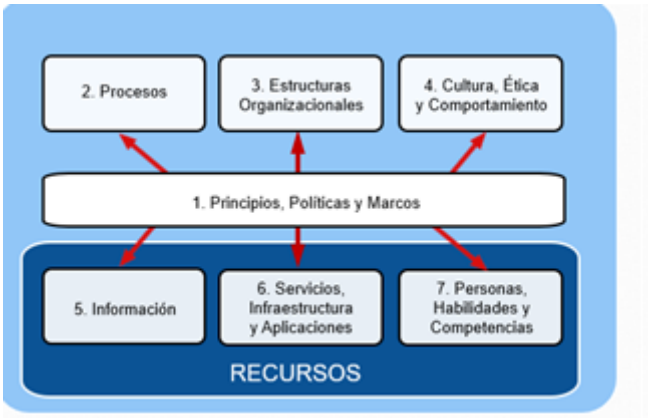

Fig. 2. Habilitadores de CoBIT 5.0
Fuente: CoBIT 5.0 ® 2012 Fig.12, ISACA All Right Reserved

Es importante tener en cuenta la convergencia Sarbanes-Oxley frente a CoBIT 5.0 ya que, requiere estrictamente que se incluya en la gerencia un informe de control interno en cada presentación como se evidencia en la Fig.2, en donde se muestren las siguientes recomendaciones:

- Se debe establecer la responsabilidad de la administración para establecer y mantener una acorde estructura de control interno y procedimientos debidamente estructurados para la información financiera.
- Esta información a su vez, debe contener una evaluación a partir del año fiscal más reciente por parte de la organización y de este modo garantizar la efectividad de la estructura y los procedimientos de control interno.
- La convergencia Sarbanes-Oxley frente a CoBIT 5.0 se debe realizar de forma controlada y en la cuál se conozca por parte de todas las áreas operativas de la organización, de tal forma que garantice unas estrictas recomendaciones de un marco de referencia, hacia una ley de estricto cumplimiento.

III. GOBIERNO Y ADMINISTRACIÓN

Dentro de las características indispensables para la convergencia CoBIT 5.0 frente a Sarbanes-Oxley, se requiere tener el gobierno definido en la organización, ya que este asegura el logro de los objetivos, al evaluar todas las necesidades de las distintas partes, se debe revisar las condiciones y opciones fijando directivas al momento de tomar decisiones; en este caso sería fundamental monitorear el desempeño cumplimiento y progreso del mismo, comparándolos con las metas propuestas de cada estructura organizacional.

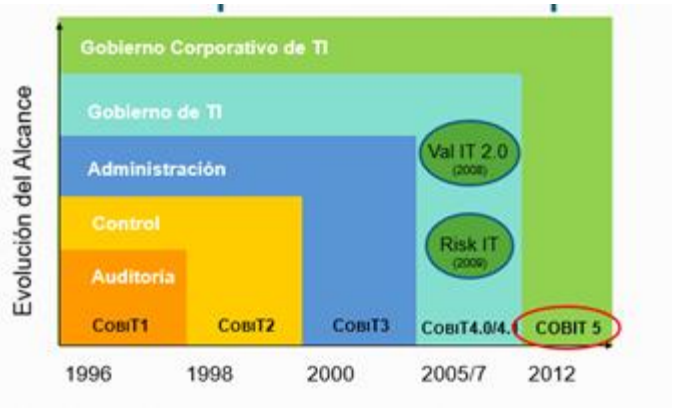

Fig. 3. Marco empresarial completo.
Fuente: CoBIT 5.0 ® 2012 ISACA All Right Reserved

También, la administración planifica como se describe en la Fig.3, construye y monitorea de forma continua las actividades presentadas conforme a las decisiones de la alta gerencia fijadas por el gobierno para así lograr los objetivos de la organización en su totalidad.

Dando alcance al gobierno y organización CoBIT 5.0, lo que propone es unir los cinco principios de tal manera que permitan a la organización construir un marco efectivo de gobierno y administración basado en una base de siete habilitadores, mencionados anteriormente; los cuáles optimizan la inversión en tecnología e información, así como su uso en beneficio de las partes interesadas que mejoran la inversión en tecnología e información.

El marco empresarial completo de CoBIT 5, presenta grandes fases a lo largo de los años en dónde se han implementado distintas áreas de conocimiento que van desde 1998 hasta el año 2012 en el cuál se describen a continuación:

- CoBIT 1: En el año 1996; implemento auditoría para revisorías fiscales y tener control de los procesos internos y externos de la organización.
- CoBIT 2: Incursionaron en el año 1998 con el tema de objetivos de control y controles en dónde se verificaba que todo se esté cumpliendo a cabalidad según la organización o ámbito que se tenga.
- CoBIT 3: Luego en el año 2000 CoBIT 3 incluye el tema de administración de activos y no activos según la clasificación que otorga a la organización para el correcto uso de los mismos, además en el tema de administración externo e interno de proveedores.
- CoBIT 4: Llega después de cinco años y siete años con su versión mejorada la 4.0 la cuál ya adiciona el control de riesgo de tecnologías de la información incorporado en el año 2009, la valoración de TI 2.0 de 2008 el cuál permite asociar todo el tema de gobierno de TI, administración y gobierno dentro de la alta dirección, estableciendo parámetros concretos en el marco empresarial.
- CoBIT 5.0: La versión más completa con múltiple información asocia en el año 2012 el tema de gobierno corporativo de TI y gestión de seguridad de la información en todas las ramas y áreas de responsabilidad en la por otra por otra parte, la organización, permite de forma definida analizar y dar alcance al gobierno de las organizaciones a nivel mundial.

Además, entender de forma adecuada los marcos de referencia, ayudara a la compañía a utilizar CoBIT 5.0 de forma efectiva para hacer de forma ordenada y realizar mejores inversiones y a su vez tomar mejores decisiones en relación con TI.

Se debe generar un valor a partir de su información y sus propios activos tecnológicos, esto con el fin de ayudar a todas las empresas, y a su vez todos estén alineados hacia la misma dirección, dentro de los principios recopilados en la nueva guía CoBIT 5.0 son:

- Satisfacer necesidades de los colaboradores: Lo más difícil y crítico es vincular y asociar los objetivos del negocio con los objetivos de TI, ya que se presenta conflicto de intereses al no tener claro el marco de referencia que se debe adquirir para logar un apoyo frente a la alta dirección.
- Mantener y cubrir la empresa de extremo a extremo: Hoy en día las compañías deben cambiar su visión y deben adaptarse a nuevas formas o estrategias de como lograr mantener alineados sus objetivos de considerar al área de TI como un activo más y no cómo un costo. Esto radica principalmente en la alta dirección, asimismo a su vez deben tomar la responsabilidad de gobernar y gestionar los activos fijos dentro de sus propias funciones y responsabilidades.
- Aplicar un marco integrado: Es indispensable utilizar un sólo marco de gobierno, el cuál debe ayudar y brindar a las organizaciones un amplio valor de los activos y recursos de sistemas.
- Separar gobierno de la administración: Todos los procesos de gobierno aseguran de forma eficaz que los objetivos se alcancen mediante una evaluación rigurosa de las necesidades de los interesados, el establecimiento de la dirección a través de la categorización y la toma de decisiones; y el monitoreo del desempeño, el cumplimiento o progreso. Se debe tener los resultados de las actividades de gobierno, la administración de la organización y de TI, es necesario planear, realizar,
- Crear y monitorear: las actividades para que se asegure el alineamiento con la alta dirección que se estableció.

Se debe comprender las diferentes estructuras organizacionales las cuales cumplen distintos propósitos dentro de la estructura de gobierno, además liderazgo del presidente, alineado a la junta directiva, es decir: el gobierno debe asegurar que se evalúen las necesidades de las partes interesadas, así como las condiciones y opciones, para determinar los objetivos claros y corporativos balanceados acordados a lograr; igualmente fijar directivas al establecer prioridades y mandatos y tomar decisiones; y de este modo poder monitorear el desempeño, cumplimiento y progreso comprándolos con los objetivos fijados.

De este modo, la administración planifica, construye, lleva a cabo y monitorea las actividades conforme a las directivas fijadas por el gobierno, y así lograr los objetivos de la compañía, CoBIT 5.0 no es obligatorio, es solo un marco de referencia, pero propone que las empresas implementen los procesos de gobierno y administración de tal manera que las áreas claves de las estructuras organizacional, queden cubiertas, tal cuál cómo se muestra a continuación en la Fig.4:

Fig. 4. Estructura de gobierno.
Fuente: Facilitadores, Chae2015 WordPress

IV. MARCO DE REFERENCIA

El marco de negocio en las organizaciones es fundamental, para lograr la convergencia frente a las leyes de hoy en día, en especial Sarbanes-Oxley.

La distinción entre gobierno corporativo y gestión queda lista y clara en CoBIT 5.0 se encuentra siempre alineada con la ISO 38500 la cuál permite una adopción con múltiples variaciones.

CoBIT 5.0, no necesita procedimientos, lo cuál lo hace libre para implementarlo en cualquier organización. Este a su vez señala resultados deseables y ofrece métodos y métricas. Según ISACA, este no es un modelo radical sino tolerante e incluso recomienda otras normas o marcos (como ISO 27001 o ITIL en cualquiera de sus versiones), Con los que propone una alineación de manera que la organización procede a adoptar para sus procesos, este marco de referencia establece su propio sistema de gobierno y administración de TI.

La guía de buenas prácticas CoBIT 5.0, se adhiere al tema de gobierno de TI y es apoyado por múltiples iniciativas y legislaciones a nivel mundial entre esas, Sarbanes-Oxley, alterna con temas de tecnologías de la información en auditorias previas de clase; interna y externa relacionándose las dos y creando un marco sólido para empresas que cotizan en la bolsa de valores de New York.

Fig. 5. Modelo de referencia de procesos
Fuente: BITCompany, ISACA 2012®

El marco se ha desarrollado de acuerdo a las necesidades de los interesados, estas a su vez abstraídas como resultado de amplias encuestas mundiales y múltiples bases de datos que dan testimonio de las organizaciones la cuál utilizan hoy en día, es por eso que la Fig.5, describe la alineación estrategia, la entrega de valor, administración de riesgos, administración de recursos y medición del desempeño en el gobierno de TI.

Su marco de referencia propone siete categorías de elementos denominados habilitadores, en la versión española están altamente interrelacionados para construir el sistema específico de gobierno y gestión según la necesidad.

CoBIT 5.0, se basa en cinco principios que son:

1) Procesos.
2) Cultura, ética. comportamientos.
3) Estructuras organizativas.
4) Información.
5) Principios y políticas.
6) Habilidades y competencias.
7) Capacidades de servicio.

Dentro de su marco referente integra material previo de CoBIT 5.0 y de ISACA. Y a su vez fuente de terceras partes que ayudan a dar un mayor grado de sostenibilidad, su estructura es sencilla y facilita la integración de cualquier marco o norma que se encuentre disponible, este propone un modelo de referencia de procesos y se rige por la persecución del valor para quienes necesitan seguir las indicaciones.

Esta estructurado en procesos de gobierno corporativo de gestión de administración, diferenciados y relacionados entre sí. Como se menciona anteriormente en los siete principios o habilitadores que se necesita para crear valor.

CoBIT 5.0, consta de un marco de gobierno de TI como se describe en la Fig.7, donde requiere: requisitos corporativos, normas de industria y regulación del entorno frente a la gestión del riesgo y gestión de recursos.

Fig. 6. Gobierno TI empresarial
Fuente: **Tcp USTGlobal®, ISACA**

V. IMPLEMENTACIÓN

Para la implementación del CoBIT 5.0 es necesario tener presente los siguientes asuntos:

CoBIT 5.0: Implementación cubre las siguientes líneas de conocimiento:

1) Posicionamiento del gobierno de TI en la organización.
2) Adopción de los primeros pasos para mejorar gobierno empresarial de TI.
3) Factores de éxito y retos para la implementación.
4) Habilitación del cambio de comportamiento y organizacional relacionado con el gobierno empresarial de TI.
5) Implementación de una mejora continua que incluye la habilitación del cambio y la gestión del programa.
6) Uso de CoBIT 5.0 y sus principales componentes de marco de referencia a nivel mundial.

De esta forma, ISACA ha desarrollado el marco de CoBIT 5.0 para ayudar a las compañías a implementar los llamados habilitadores de gobierno. De hecho, la implementación de un buen gobierno corporativo de TI es casi imposible sin la activación de un marco efectivo de gobierno. También están disponibles las mejores prácticas y los estándares que soportan al CoBIT 5.0.

Los marcos de referencia y normas son útiles solamente si son adoptados de manera efectiva. Hay que superar muchos retos y resolver varios asuntos para poder implementar un gobierno empresarial de TI de manera exitosa, por ello la información y la presencia general de cualquier área de la organización ocupan cada día una parte importante en todo aspecto de la vida comercial y pública.

Por ello, es fundamental generar más valor de las inversiones en la tecnología y de administrar una gama creciente de riesgos relacionados con la Tecnología, nunca ha sido mayor que ahora, pero se puede lograr alineando todas las áreas.

Por otra parte, debe haber una regulación y legislación cada vez más estricta sobre el uso comercial de la información también impulsa una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, el marco de referencia realiza siete preguntas como se refiere la Fig.7, la cuál muestra los pasos para sostener y crear valor.

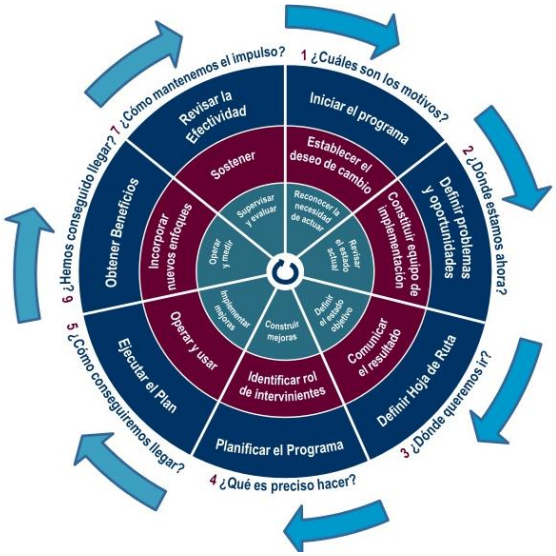

Fig. 7. Implementación CoBIT 5.0
Fuente: ISACA 2012. All Right reserved

VI. CONVERGENCIA SARBANES-OXLEY FRENTE A COBIT 5.0

Dentro del marco legal la ley Sarbanes-Oxley, fue aprobada en julio de 2002, después de un gran debate fuerte y directo en la cámara de representantes de USA.

La convergencia que se da principalmente en mejorar de forma radical la protección a los accionistas a través de una amplia gama de medidas, muy estrictas y exigentes dentro del gobierno de TI, incorporando a los diferentes empleados de la organización, cubre toda su amplia estructura de los bancos de inversión, en los profesionales financieros, así como de formar parte importante la actividad y regulación de los auditores o responsables de las cuentas y obligaciones y responsabilidades de los involucrados en empresas que cotizan en el mercado de bolsa de valores, dentro de sus principales contenidos que incorporan seis grandes áreas de conocimiento:

1) La mejora en la calidad de la información pública que se está transmitiendo y en la estructura de la misma.
2) Responsabilidades de gobierno corporativo de las sociedades que están internamente implicadas con los datos y control financiero.
3) Mejora considerable en las conductas éticas exigibles, este implica mayor exigencia y responsabilidad en manejo indebida de información confidencial, así como su divulgación a terceros.
4) Demanda mayor responsabilidad en supervisión de los mercados cotizados.
5) Se incrementa la autoridad que sanciona a incumplimientos asociados a temas de corrupción y desfalcos.
6) El gran aumento de exigencias y presión sobre la total autonomía de los auditores ya sean externos o internos, el cuál garantice que todo se controle y se actué con diligencia frente a distintas áreas de la organización.

Se logra incorporar mayor control frente a la información pública presentada a la junta directiva, el cuál se debe llevar con informes trimestrales y anuales en donde se garantice que todo esté en orden y sin estar alterada, al igual los controles sobre la información que se envía al mercado debe ser garantizada por la eficiencia del control interno sobre la misma.

Se deberá disponer de una buena metodología y capacidad de compensación al auditor el cuál suplan y permitan ejecutar el desarrollo transparente de sus actividades frente a cualquier escenario que se presente.

Asimismo, emitidas por las empresas es de gran valor, el endureciendo de los controles financieros, se evidencia la ley Sarbanes-Oxley como una alterativa de estricto cumplimiento para tener un control específico de las cuentas

anuales y todos los informes financieros que se tengan que emitir frente a los distintos procesos que se integran en el gobierno de TI y gestión de administrativa que propone CoBIT 5.0 al estar alineados de forma integral con la seguridad informática, con el monitoreo de la contabilidad y así sancionar a los profesionales o ejecutivos que incurran en fraudes corporativos dando gran relevancia a múltiples auditores calificados para su labor.

La información pública presentada deberá ser legitimada por los directivos de la sociedad, es decir, los directivos tendrán que asumir la responsabilidad y hacer las correcciones indicadas de acuerdo a algunos parámetros los cuales son:

Las buenas prácticas de hacer convergencia Sarbanes-Oxley frente a CoBIT 5.0, es desarrollar un marco dentro de gobierno de TI bajo la legislación financiera, de este modo reduciendo el índice que pueda ocasionar corrupción y fuga de datos dentro de la organización, debido a que CoBIT 5.0 plantea temas concretos de garantizar la seguridad de la información.

Dentro del marco legal existen algunos factores claves en donde se puede ver involucrado la corrupción, esto en el contexto financiero puede ocasionar grandes desfalcos y fraudes en las organizaciones, hoy en día si no se tiene una convergencia de gobernó de TI alineado a la dirección y un control estricto para salvaguarda las inversiones globales de los accionistas, puede causar una serie de desastres irremediables, por lo tanto es necesario tomar las medidas necesarias y hacer una convergencia Sarbanes-Oxley frente CoBIT 5.0 para garantizar todas las áreas de responsabilidad de las organizaciones.

Debe haber un dialogo donde se evidencia la comunicación de una forma adecuada entre los auditores y el comité de auditoría de los errores o fraudes que se pueden presentar en las organizaciones.

Además, se harán verificaciones sobre la información suministrada al mercado, de igual forma el control interno sobre la misma.

También, se hará una valoración del control interno, el cuál tendrá el permiso de la dirección de la sociedad y se evaluado por el auditor de cuenta, el cuál es el encargado de la corrección de lo manifestado por la sociedad.

Se deberá establecer un canal unificado, donde se puedan hacer las respectivas denuncias a fraudes o desfalcos que se pueda presentar en la organización, asimismo se brindar una protección de seguridad a los denunciantes de este tipo de irregularidades.

Se adecuará algunas restricciones para el proceso de contrato de personal del grupo de auditoría.

La calidad de la información es uno de los pilares de las reformas propuestas por Sarbanes-Oxley, los datos que se presentan deben ser un apoyo incondicional para salvaguardar cualquier dato adyacente de la organización, igualmente la calidad de la auditoria debe ser un factor clave.

De este modo, Sarbanes-Oxley de forma directa o indirecta ha establecido algunos parámetros eficaces de auditoría más concretos y exigentes con el fín de evitar el fraude financiero, es así como se tiene una mayor responsabilidad por parte auditor a cargo del proceso en el cuál se pueden considerar tres pilares fundamentales al momento de la convergencia de Sarbanes-Oxley frente a CoBIT 5.0, es principalmente su alineamiento con normas técnicas como ISO27002 e ITIL, cada una de ellas aportando componentes que se convertirán en controles que se van a evidenciar a lo largo del proceso, y finalmente se desarrollara flujos y se identificaran controles dentro de estos mismos los cuales permitirán la generación de evidencias al momento de presentar cualquier informe antes la alta dirección y a los accionistas en general.

Fig. 8. Gobierno corporativo y ley sarbanes-Oxley.
Fuente: Telefónica S.A

Otro aspecto relevante que se debe tener en cuenta al momento de realizar la convergencia es la prohibición total del auditor para que verifique los procesos de su misma cuenta, ya que este solo puede prestar determinados servicios a sus clientes que no pertenezcan a su grupo, es por eso que la Fig.8, describe de una forma concreta el modelo de control interno frente a la Ley-Sarbanes-Oxley.

Se aplicarán algunas restricciones primordiales para que una entidad contrate personal calificado al momento de realizar la requisición trimestral de acuerdo a los parámetros de ley Sarbanes-Oxley, se realiza con el fin de garantizar en los auditores la mínima desviación al momento de dar su veredicto como punto a favor y así se preste para fraude dentro de la organización.

Por otra parte, se hará una auditoría correctamente realizada frente a temas de control interno, es indispensable conocer todos los procesos de gobierno y administración de TI, debido a que este procedimiento brinda confianza y seguridad para toda la organización en el cuál se alinea

correctamente con los objetivos principales de todas las áreas de negocio.

Las personas a cargo de designar, retribuir y supervisar al auditor serán los directores.

Tendrá que haber expertos financieros en el comité de auditorías, y la información será únicamente de quienes son los consejeros con esta experiencia.

Según lo planteado, esta ley tendrá un impacto directo en el desempeño del auditor, así desde la interlocución más concreta y honesta con los comités de auditoría, hasta la creación de un regulador específico para esta.
Las operaciones realizadas por los agentes que pueden adquirir información confidencial no pública, están sometidas
a una exigencia de información a tiempo muy corto y de forma veraz,

Dentro de la convergencia Sarbanes-Oxley frente a CoBIT 5.0, se describe la administración de activos dentro de la organización, todo tiene que estar documentado dentro del marco de buenas prácticas hasta el tema de referencia legal, esto busca reducir el índice de desfalcos y corrección frente a los empleados internos, se debe tener en cuenta los controles que se requieran implementar del marco de referencia, cabe destacar que el tema de convergencia aplica en todas las áreas del negocio, dando como referencia y seguridad la legislación en empresas que cotizan en la bolsa de valores de New York.

Esta ley pretende mejorar la protección de los accionistas frente a temas financieros y revisoría fiscal, ampara y salvaguarda las acciones o inversiones que se dan dentro de la organización; teniendo en cuenta un control frente a una trazabilidad preestablecida según la ley Sarbanes-Oxley, es donde el gobierno y la tecnología muestran en la Fig.9, las normativas de riesgo en el ámbito de entes de control y mercado.

Fig. 9. Normativas del riesgo y cumplimiento TIC.
Fuente: Aspecto profesionales, José Luis Colom

Se presentan varias normativas de riesgo y cumplimiento frente a la convergencia Sarbanes-Oxley frente CoBIT 5.0, dentro de las mencionadas están las siguientes:

- COSO (Committee of Sponsoring of the Treadway Commission): Es el encargado de desarrollar una comisión voluntaria del sector privado de ESTADOS UNIDOS, encargado principalmente de la gestión del riesgo y control interno.
- PCI-DSS (Payment Card Industry Data Segurity Standard): Esta creado por las organizaciones de tarjetas de crédito y débito más importantes para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y tomar las medidas de seguridad a nivel mundial.
- NIST SP- 800 (National Institute of Standards and Technology): Es un conjunto de publicaciones del NIST (Instituto Nacional de Estándares y Tecnología), puede ser utilizado por cualquier entidad, para análisis de riesgos.
- ISO 31.000–Gestión del Riesgo: Norma internacional publicada en 2009 por ISO (Organización Internacional de Normalización), proporciona los principios y directrices genéricas sobre la gestión del riesgo para empresa pública y privada

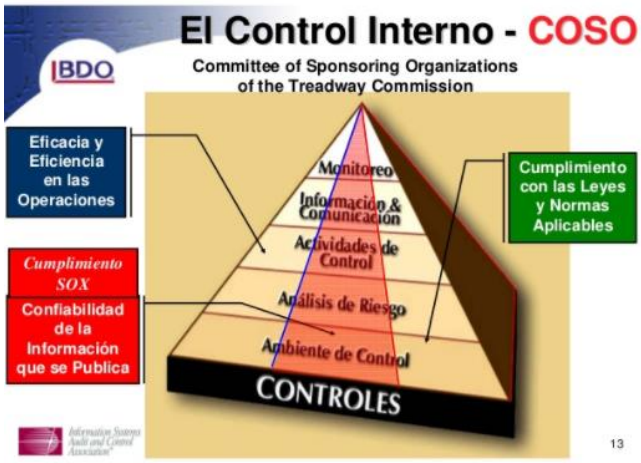

Fig. 10. Convergencia Sarbanes-Oxley & CoBIT 5.0
Fuente: IBDO, Capitulo Ciudad de México ISACA®

Dentro de los conceptos y prácticas para la gestión de servicios de las tecnologías de la información y las operaciones de gobierno de TI, se ven involucrados todos los marcos de referencia, como se muestra a partir de la pirámide de controles y monitoreo mostrado en la Fig.10, el cuál tiene relación directa con CoBIT 5.0, por el tema de mejora continua y desarrollo de gobierno de administración de TI, esto transversal a la Ley Sarbanes-Oxley.

Cuando se tiene en cuenta la mejora continua del servicio, simplemente se alinea el gobierno y administración de TI frente a legislación, dado que representa una estructura sólida en ambas partes y a su vez se alineen en el ámbito útil de generar valor para la organización.

Todos los marcos de gestión de servicios de TI, aseguran de forma eficiente frente a sus controles y su mejora continua en los procesos, dentro de su fase organizacional de la organización.

Cabe destacar que cada una de estas metodologías no son obligatorias, es un marco de referencia o guía de buenas prácticas para realizar todos los procesos en TI.

También ofrece métodos de control y mejoras para los servicios y productos que se encuentra en la etapa productiva, entonces la ayuda que ofrece frente a la convergencia es su apoyo hacia la estrategia, diseño, transición, operación y mejora continua del servicio el cuál relaciona notablemente con CoBIT 5.0 para ayudar a las organizaciones a crear un valor óptimo a partir de TI y de esta forma mantener un equilibrio en la parte legal frente a la Ley Sarbanes-Oxley.

Fig. 11. ITIL
Fuente: BITCompany Starting Point. ISACA®

Se tiene en cuenta todas las normativas de cumplimiento de TI la cuál administra adecuadamente los riesgos, en este caso de temas Operativos, legales, seguridad, Continuidad, se relaciona abiertamente con los accionistas y personal involucrado en salvaguardar los inversionistas de cualquier clase de fraude o desfalco fiscal utilizando el marco descrito en la Fig.11, en el cuál los controles Sarbanes-Oxley implementados permiten el cumplimiento de más de una normativas, y de esta forma también permiten mitigar los riesgos existentes que se ven involucrados por no tener un gobierno y administración de TI definido.

Además, es necesaria la centralización de los controles de estricto cumplimiento para evidenciar el cumplimiento de más de una normativa, así como su específica utilización de cualquiera de los riesgos analizados e identificados.

Lo que en si requiere Sarbanes-Oxley es una certificación de la administración acerca del control interno de la compañía, acompañado de múltiples reportes de control internos en información financiera, esta acta incluye varias secciones, las cuáles se especifican varias finalidades específicas.

Algunas de las secciones clave y fundamentales son:

- Sección 302: Los directivos de la compañía deben hacer representaciones relacionadas con la confidencialidad de la información y de los controles, procedimientos y aseguramiento contra el fraude.
- Sección 404: Los directivos deben proveer una evaluación anual de la efectividad de los controles internos para el reporte de la información financiera, y de esta forma obtener una certificación garantizada de los auditores externos quienes garantizan que los controles son efectivos.

Es indispensable al momento de realizar la convergencia en la organización se adopte un marco de control interno, cómo se menciona anteriormente, El marco de referencia para gestión de control interno el cuál define un marco de control interno adaptado a CoBIT 5.0, el cuál ha tenido una gran aceptación para cumplir con la Ley Sarbanes-Oxley.

Se evidencia la efectividad en las operaciones diarias de la compañía en los cuáles brinda y se garantiza confianza del reporte financiero y cumplimiento con regulaciones aplicables en cualquier organización donde esta lo requiera, ya que es indispensable tener un marco de control interno que permita operar toda la organización de forma alterna con el gobierno y administración de TI de forma transversal, esto ayuda a reducir el desfalco y corrupción que se presenta en las organizaciones, además si se tiene una guía de buenas prácticas como ITIL, estaría mejor alineado hacia los objetivos estratégicos del negocio,

Fig. 12. Marco de control interno COSO
Fuente: Latín América CACS SM®

Se deben tener las siguientes consideraciones planteadas en la Fig.12, del marco de control interno para desarrollar una sólida estrategia y para que se pueda realizar la convergencia efectiva entre Sarbanes-Oxley y CoBIT 5.0.

- Evaluación de Riesgos: Se debe incorporar en la organización y cada área de responsabilidad en el cuál debe ser económico y operacional.
- Ambiente de Control: Es indispensable tener la disciplina y estructura definida en la organización.

- Actividades de Control: La empresa debe contar con la aprobación de la alta dirección y segmentar las funciones de cada una de las personas.
- Información y comunicación: Es un tema importante al momento de la convergencia, ya que se debe relacionar todo el contenido bajo actas y escritos, todo debe ser documentado.
- Monitoreo: Es indispensable monitorear y tener trazabilidad con respecto al tema de monitorear y verificar que se está haciendo dentro del marco de control interno.

Dentro de las múltiples características y funcionalidades que presenta la convergencia de la ley Sarbanes-Oxley establece penas corporales para los directivos que no cumplan con cualquier sección establecida en la compañía. Aunque muchas organizaciones no están obligadas a cumplir con la Ley Sarbanes-Oxley, existe hoy en día muchas tendencias a establecer leyes similares en varios países fuera de los estados unidos, inclusive en reino unido UK.

Además, en sus principios corporativos se deben tener los siguientes aspectos:

- Derechos de los accionistas frente a temas de revisoría fiscal y temas financieros.
- Tratamiento equitativo frente a los accionistas.
- El rol frente a cualquier estructura organizacional se debe tener en las partes interesadas dentro del gobierno corporativo.
- Se debe incorporar una seria de medidas en pro de la divulgación de datos y transparencia de los mismos.

El gobierno corporativo de CoBIT 5.0 converge a Sarbanes-Oxley en temas de transparencia, objetividad y equidad en el buen trato hacia los socios y accionistas de la organización, y claro está la responsabilidad directa que se tiene frente a terceras partes quienes aportan recursos.

Inicialmente y en todo momento dentro de la organización, la Ley Sarbanes-Oxley brinda una responsabilidad del CEO (Chief Executive Officer), y el CFO (Chief Financial Officer), los cuáles están a cargo de la creación de valor frente a cualquier tema financiero y gobierno.

Muchas firmas se centrarán y harán énfasis en el gobierno corporativo para cumplir con Sarbanes-Oxley y asimismo con sus objetivos de negocio.

Dentro del modelo de gobierno corporativo se enfocará en los siguientes aspectos:

- Administración y gestión del riesgo.
- Estricto cumplimiento de regulaciones.
- Administración y evaluación de resultados.

Entonces, se debe tener en cuenta previamente a los accionistas al definir todas las estrategias, igualmente dar prioridad y dirección a los procesos cuando se implementan las estrategias correspondientes, se debe asegurar insdispensablemente que los procesos den resultados, asimismo ser medidos que muestren y se informe estadisticas que garanticen y salvaguarden la relación que se tiene con los accionistas, en donde siempre esten predispuestos en el marco lde referencia CoBIT 5.0 y la Ley Sarbanes-Oxley.

Fig. 13. Estrategias y gobierno corporativo
Fuente: Latín América CACS SM®

VII. CONCLUSIONES

El buen uso de marcos de referencia en la organización, una guía de buenas prácticas y controles establecidos para la mejora continua en cada uno de los procesos dentro de cada área de responsabilidad, CoBIT 5.0 demostró tener estructurado sus procesos de gobierno corporativos de gestión administrativa de forma adecuada, diferenciados y relacionados entre sí.

Cabe destacar la ley Sarbanes-Oxley, una ley basada en hechos reales cuyos temas de entendimiento de la ley, permiten de forma rápida a las empresas identificar los riesgos claves de la información financiera y de este modo valorar su impacto sobre todas las estructuras y áreas de la organización. Además, establece una nueva conducta de responsabilidades corporativas y normas de carácter estricto para prevenir y sancionar todo fraude corporativo y actos de corrupción que se presenten.

Se evidencia en las organizaciones hoy en día está creciendo desbordadamente con respecto al comercio de valores, es donde la corrupción y el fraude detectado y la mala práctica de personal calificado quienes de forma oculta engañan a sus socios y a los mismos empleados de la organización. Es donde la ley Sarbanes-Oxley de 2002 aparece para fortalecer la regulación financiera y la actividad contable pública.

Hoy en día es fundamental realizar estas clases de convergencias con distintos marcos de referencia frente a empresas que coticen en la bolsa de valores de New York que quieren cuidar y valorar sus accionistas, para que exista

trazabilidad y no exista ninguna clase de desfalco ni mucho menos corrupción dentro de las organizaciones.

REFERENCIAS

[1] Harmon, J.E. "The Structure of Scientific and Engineering Papers: A Historical Perspective. *IEEE Trans. On Professional Communication"*. Vol 32, No. 2, (September, 1989), pp. 132-138.

[2] Roa J. CoBIT- "Control Objectives for information and related Technology". IL USA, Vol. 01, (May 2012), pp. 07- 26.

[3] Durán, J.A. COSO – CoBIT, "Aspectos comunes y aportación a los objetivos de la empresa", NL. Vol. 01, (October, 2015), pp. 02-12.

[4] George J.B, "The Quality of corporate Financial Statements and Theirs Auditors before and after Enron", Washington, DC. Vol 497, (November, 2003), pp. 14 -25.

[5] Al L. Hartgraves and George J. Benston, "The Evolving Accounting Standards for Special Purpose Entities (SPEs) and Consolidations, Accounting Horizons 16", USA, (September 2002): pp. 245–258.

[6] Morales J. Diaz, "La ley Sarbanes-Oxley y la auditoria", Vol. 169, PD, (September, 2007), pp. 104 – 109.

[7] Rosell Borox. A. "Convergencia de las normativas de riesgo y gestión integrada o como no fracasar en el intento", ISACA México, (March, 2017), Vol. 02, pp. 04 – 41.

[8] Peña Ibarra J.A. "Seguridad desde el punto de vista Sarbanes-Oxley" CACS 2006, México, Vol. 233, (Octuber, 2007), pp. 02-51.

[9] Segura González, J.A. "Adoptando los modelos de control interno COSO y CoBIT", Ciudad de México, Vol.01, (October, 2013), pp.03- 41.

[10] ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3.ª edición, EE. UU., 2014, Available on the -Website, www.isaca. org/Knowledge-Center/Research/ResearchDeliverables/ Pages/ITAF-3rd-Edition.aspx

[11] Kerr, D. S., & Murthy, U. S. (March,2013). "The importance of the CoBIT framework IT processes for effective internal control over financial reporting in organizations: an international survey. Information & Management", 50(7), pp.590-597.

AUTOR

Joan Sebastián Niño, nació en la ciudad de Bogotá, Colombia. Se gradúo en la Universidad Los Libertadores de ingeniero de sistemas, actualmente se encuentra culminando la Especialización en Seguridad Informática Universidad Piloto de Colombia, es certificado en ITIL V3 Foundations 2011.

El ingeniero Niño, posee gran experiencia en el tema investigativo, se encuentra vinculado al programa de semilleros de investigación "Epsilom" de la Universidad Los Libertadores, en el cuál desarrollo múltiples proyectos dando finalizado sus tres módulos del grupo en mención, bajo la dirección del Ing. Javier Daza P. Coordinador de Egresados de la facultad de Ingeniería de Sistemas Universidad Los Libertadores.

"Este documento está diseñado con fines educativos e investigativos. Es solo una guía práctica para adaptar a cualquier necesidad".